General Data Protection Policy

Document Owner:	Ruedi Baumann
Version:	Version 1.0
Approved Date:	3 November 2021
Review Date:	3 November 2022

Table of contents

1. Introduction 1
2. Background 1
3. Policy Statement 1
4. Roles and Responsibilities 2
5. Data Protection Principles 3
6. Data Subject Rights 5
7. Basis of Processing 6
8. Security 6
9. Disclosure 6
10. Retention 7
11. Data Transfers 7
12. Personal Data Breaches 8
13. Disciplinary Action 8

Appendix 1 – UK GDPR Definitions 9

1. Introduction

1.1 This policy covers all activities of Jesus College (''the College''), where personal data is controlled or processed as defined by the Data Protection Act 2018 ("DPA 2018") and the UK General Data Protection Regulation ("UK GDPR").

1.2 Protecting personal data is vital not only to maintain the trust placed in the College by its stakeholders but also to demonstrate the College's commitment to data protection. As such, adherence to this policy and its intent is a mandatory obligation for the College's Governing Body, Trustees, employees, students, consultants, and contractors (hereafter "staff and students").

1.3 Should the College's Governing Body come to the view that data held by the College falls out of the scope of this policy, then written confirmation of such must be obtained from the Data Protection Officer (DPO) in advance of any potential divergence from full adherence to this policy. The DPO will lead on such discussions.

2. Background

2.1 Background: The UK GDPR supersedes the EU General Data Protection Regulation ("EU GDPR") (EU Regulation 2016/679), on the protection of natural persons relative to the processing of personal data and on the free movement of such data. The purpose of the UK GDPR is to protect the "rights and freedoms" of natural persons (i.e. living individuals) by ensuring that data controllers are accountable for ensuring that personal data is processed in accordance with the six data processing principles.

2.2 Material scope: The UK GDPR applies to the processing of personal data wholly or partly by automated means (e.g. by computer) and to the processing other than by automated means of personal data (e.g. paper records), which form part of a filing system or are intended to form part of a filing system.

2.3 Territorial scope: The UK GDPR applies to all data controllers established in the UK that process the personal data of data subjects, in the context of that establishment. It also applies to controllers and processors outside of the UK who process personal data to offer goods and services or monitor the behaviour of data subjects resident in the UK.

2.4 Terminology: A comprehensive list of terms used in the UK GDPR is at Appendix 1.

3. Policy Statement

3.1 The College is committed to compliance with all relevant UK laws in respect of personal data and to protecting the "rights and freedoms" of individuals whose information has been collected and processed in accordance with the UK GDPR.

3.2 Compliance with the UK GDPR is described by this policy and other relevant policies, along with connected processes and procedures.

3.3 This policy applies to all College staff and students wherever they work. Any breach of the UK GDPR will be dealt with under the 'Disciplinary Policy'.

3.4 The UK GDPR and this policy apply to all personal data processing functions, including those performed on personal data relating to staff and students, and any other personal data which the College processes from any source e.g. service users.

3.5 The DPO shall ensure that the Record of Processing Activities ("RoPA") is reviewed annually in light of any changes to the College's processing activities and for any additional requirements identified by means of any data protection impact assessments ("DPIA") to be given affect as necessary or appropriate.

3.6 Partners and any third parties working with or for any part of the College and who have or may have access to personal data, will be expected to have read, understood and to comply with this policy.

3.7 No third party may access personal data held by the College without having first entered into non-disclosure agreement (NDA) which imposes on the third party obligations no less onerous than those to which the College is committed, and which gives the College the right to audit compliance with the NDA.

4. Roles and Responsibilities

4.1 The College is the data controller and/or data processor as defined in the UK GDPR.

4.2 The Governing Body and all those in managerial or supervisory roles throughout the College are responsible for developing and encouraging good information handling practices within their respective areas of responsibility.

4.3 The responsibilities for managing this procedure are further set out in individual job descriptions, the Information Security Policy ("ISP") and Individual User Agreements.

4.4 The DPO is accountable to the Governing Body for the management of personal data within the College and for ensuring that compliance with data protection legislation and good practice can be demonstrated. This accountability includes:

a. Development and implementation of the UK GDPR as required by this policy; and

b. In cooperation with the DPO, the resolution of any issues raised by the College's security and risk assessment process that may impact upon compliance with this policy.

4.5 The DPO, whom the Governing Body considers to be suitably qualified and experienced, has been appointed to take responsibility for the College's compliance with this policy on a day-to-day basis and has direct responsibility for ensuring the College complies with the UK GDPR, as do all staff and students, in respect of the data processing that takes place within their respective areas of responsibility.

4.6 The DPO has responsibilities in respect of procedures such as the Data Subject Access Request Procedure and s/he is the first point of call for staff and students seeking clarification on any aspect of data protection compliance.

4.7 Compliance with data protection legislation is the responsibility of all staff and students who process personal data.

4.8 The College's new joiner and induction process sets out specific training and awareness requirements in relation to specific roles and staff and students generally.

4.9 Staff are responsible for ensuring that any personal data about them, and supplied by them to the College, is accurate and where necessary, kept up to date.

5. Data Protection Principles

5.1 All processing of personal data must be conducted in accordance with the data protection principles as set out in Article 5 of the UK GDPR and as detailed below. The College's policies and procedures are designed to ensure compliance with the principles. Individual policies and procedures define the responsibilities of staff and students in respect to their accountabilities.

5.2 Principle 1: Personal data must be processed lawfully, fairly and transparently.

5.2.1 Lawful: Identify a lawful basis before you can process personal data. These are often referred to as the "conditions for processing", for example consent or legitimate interests.

5.2.2 Fairly: For processing to be fair, the data controller has to make certain information available to the data subjects as practicable. This applies whether the personal data were obtained directly from the data subjects or from other sources.

5.2.3 Transparency: The UK GDPR includes rules on giving privacy information to data subjects in Articles 12, 13 and 14. These are detailed and specific, placing an emphasis on making privacy notices understandable and accessible. Information must be communicated to the data subject in an intelligible form using clear and plain language. The specific information that must be provided to the data subject must, as a minimum, include:

a. the identity and the contact details of the controller, joint controller and DPO and, the controller's representative (if appointed under Article 27);

b. the purposes of the processing for which the personal data are intended as well as the legal basis for the processing;

c. the period for which the personal data will be stored;

d. the existence of the rights to request access, rectification, erasure of their data, or to restrict processing or to have their data ported to another data controller or to object to the processing, and the conditions (or lack of) relating to exercising these rights, such as whether the lawfulness of previous processing will be affected;

e. the categories of personal data concerned;

f. the recipients or categories of recipients of the personal data, where applicable;

g. where applicable, that the controller intends to transfer personal data to a recipient in a third country and the level of protection afforded to the data;

h. any further information necessary to guarantee fair processing.

5.3 Principle 2: Personal data can only be collected and processed for specific, explicit, and legitimate purposes and not further processed in a manner which is incompatible with the purpose for which it was originally collected.

5.4 Principle 3: Personal data must be adequate, relevant, and limited to what is necessary.

5.4.1 The DPO is responsible for ensuring the College does not collect information which is not strictly necessary for the purpose for which it is obtained.

5.4.2 All data collection forms (electronic or paper-based), including data collection requirements in new information systems, must include a privacy notice or link to a privacy notice that is approved by the DPO.

5.4.3 On a regular basis, the DPO will review all data collection methods to ensure that the collected data continues to be adequate, relevant and not excessive.

5.5 Principle 4: Personal data must be reasonably accurate, kept up to date in the context of the purposes for which it was collected, and retained in accordance with the 'Record Retention & Disposal ("RR&D") Policy' and associated 'Record Retention & Disposal ("RR&D") Schedule'.

5.5.1 Data stored by the College must be reviewed and updated, as necessary. No data should be kept unless it is reasonable to assume that it is accurate.

5.5.2 The DPO is responsible for ensuring that all staff and students are trained appropriately in the importance of collecting accurate data and maintaining it.

5.5.3 It is everyone's responsibility to ensure that data held by the College is accurate and up to date.

5.5.4 Any changes in circumstance are to be notified to the College to enable personal records to be updated accordingly. It is the responsibility of the College to ensure that any notification regarding change of circumstances is recorded and acted upon.

5.5.5 The DPO is responsible for ensuring that appropriate procedures and policies are in place to keep personal data accurate and up to date, taking into account the volume of data collected, the speed with which it might change and any other relevant factors.

5.5.6 On at least an annual basis, the DPO will review the retention dates of all the personal data processed by the College and will identify any data that is no longer required in the context of the registered purpose. This data will be securely deleted/destroyed in line with College procedures.

5.5.7 The DPO is responsible for responding to requests for rectification from data subjects within one month. This can be extended to a further two months for complex requests.

5.5.8 If, for legitimate reasons, the request is denied, the DPO must respond to the data subject to explain the reasoning and inform the data subject of their right to complain to the UK's Information Commissioner's Office (ICO) and to seek judicial remedy. This activity does not preclude normal data quality improvement actions that are managed under business as usual.

5.5.9 The DPO is responsible for making appropriate arrangements, where third-party organisations may have been passed inaccurate or out-of-date personal data, to inform them that the information is inaccurate and/or out of date and is not to be used to inform decisions about the individuals concerned, and for passing any correction to the personal data to the third party where this is required.

5.6 Principle 5: Personal data processed must be kept for no longer than is necessary for the purpose for which it is processed.

5.6.1 Where personal data is retained beyond the period defined within the RR&D Schedule, it will be minimised, encrypted or pseudonymised, where possible, to protect the identity of the data subject in the event of a data breach. Prior to this happening a lawful basis to do so must be established and approved by the DPO, see section 5.6.3.

5.6.2 Personal data will be retained in line with the RR&D Schedule and, once its retention date is passed, it must be securely destroyed as set out in the 'Secure Disposal Procedure'.

5.6.3 The DPO must specifically approve any data retention that exceeds the retention periods defined in RR&D Schedule and must ensure that the justification is identified clearly and in line with the requirements of the data protection legislation. This approval must be in writing.

5.7 Principle 6. Personal data must be processed in a manner that ensures appropriate security.

5.7.1 Where necessary, the DPO will ensure a risk assessment is completed taking into the account the processing operations of the College.

5.7.2 In determining the appropriateness of the processing, the DPO should also consider the extent of possible damage or loss that might be caused to staff and students if a security breach occurs, the effect of any security breach on the College and any likely reputational damage, including the possible loss of public trust.

5.7.3 The College's compliance with this principle is contained in its Information Security Management System ("ISMS"), which has been developed in line with ISO/IEC 27001:2013. The general requirements of the ISMS are documented in the ISP.

5.8 Accountability. As a data controller, the College must be able to demonstrate compliance with the six data processing principles as detailed above. To this end, the DPO shall ensure that this policy is reviewed annually by the Board. This review shall determine the ongoing suitability of the policy, that the policy is deployed effectively throughout the College, and that adequate resources are available to ensure its ongoing effectiveness.

6. Data Subject Rights

6.1 Data subjects have the following rights regarding data processing, and the data that is recorded about them:

- Right to be informed – Article 12.
- Right of access – Article 15.
- Right to rectification – Article 16.
- Right to erasure (right to be forgotten) – Article 17.
- Right to restrict processing – Article 18.

- Right to data portability – Article 20.
- Right to object – Article 21.
- Rights in relation to automated decision making and profiling – Article 22.

6.2 The College is mandated under Article 12 of the UK GDPR to facilitate the rights of data subjects, for instance, responding to subject access requests (SAR); the process for doing so is described in the 'Data Subject Access Request Procedure'.

7. Basis of Processing

7.1 The College will determine the appropriate lawful basis of processing for all personal data obtained directly or indirectly from data subjects, including students.

7.2 Data subjects will be informed of the purpose for processing using the 'Privacy Notice' published on the College's website or by similar means.

7.3 Where personal data is obtained from third parties, the data subject will be sent a notice in compliance with Article 14 of the UK GDPR.

7.4 Where a special category of personal data, as defined by Article 9 of the UK GDPR, is processed, this shall be for one of the defined 10 exceptions as defined in Article 9.

8. Security

8.1 All staff and students are responsible for ensuring that any personal data which the College holds, and for which it is responsible, is kept secure and is not, under any conditions, disclosed to any third party unless that third party has been specifically authorised to receive the personal data and, where required, signed an NDA.

8.2 As part of their induction process, new staff and students, at all levels, are given guidance on where this policy and associated documents can be found on the Intranet/College's Website. Their need to comply with this policy is to be recorded.

9. Disclosure

9.1 The College is under a lawful obligation to ensure that personal data is not disclosed to unauthorised third parties which includes family members, friends, government bodies, and in certain circumstances, the police, without a legitimate purpose for doing so.

9.2 All staff and students should exercise caution when asked to disclose personal data, held on another individual, to a third party, and will be required to attend specific training that enables them to deal effectively with the risk associated with any such disclosure of personal data.

9.3 Notwithstanding the foregoing it should be borne in mind that the disclosure of information is relevant to, and necessary for, the conduct of normal College business.

9.4 Requests to provide data for one of these reasons must be supported by appropriate paperwork and all such disclosures must be specifically authorised by the DPO.

10. Retention

10.1 The retention period for each category of personal data will be set out in the RR&D Schedule along with the criteria used to determine this period, including any statutory obligations to retain personal data. The College's data retention and disposal procedures, as set out in the 'Storage Removal Procedure' and Secure Disposal Procedure', will apply in all cases.

10.2 Personal data must be disposed of securely in accordance with the sixth data processing principle – processed in an appropriate manner to maintain security, thereby protecting the "rights and freedoms" of data subjects.

10.3 Data is to be disposed of in accordance with the Secure Disposal Procedure.

11. Data Transfers

11.1 All exports of data from within the European Economic Area (EEA) to non-European Economic Area countries (referred to in the UK GDPR as 'third countries') are unlawful unless there is an appropriate "level of protection for the fundamental rights of the data subjects".

11.2 The transfer of personal data outside of the EEA is prohibited unless one or more of the 'appropriate safeguards' apply, or the processing is carried out under an exception:

- Adequacy Decision
- Standard Contract Clauses (otherwise referred to as 'Model contract clauses')
- Binding Corporate Rules ("BCR")
- International Agreements
- Derogation e.g., transfers made with the consent of the data subject

11.3 In the absence of an adequacy decision, BCR or SCC, a transfer of personal data to a third country or international organisation shall only take place on one of the following conditions:

- the data subject has consented explicitly to the proposed transfer, after having been informed of the possible risks of such transfers for the data subject due to the absence of an adequacy decision and appropriate safeguards;
- the transfer is necessary for the performance of a contract between the data subject and the controller or the implementation of pre-contractual measures taken at the data subject's request;
- the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and another natural or legal person;
- the transfer is necessary for important reasons of public interest;
- the transfer is necessary for the establishment, exercise or defence of legal claims;

- the transfer is necessary in order to protect the vital interests of the data subject or of other persons, where the data subject is physically or legally incapable of giving consent.

12. Personal Data Breaches

12.1 Any loss/suspected loss, or any unauthorised/suspected unauthorised disclosure of personal data must be reported in accordance with the 'Personal Data Breach Policy'.

12.2 Personal data breaches, including near misses, may be reported to the ICO.

13. Disciplinary Action

13.1 All staff and students are to adhere to this policy and its intent. Failure to do so may result in disciplinary action being taken. Such action might include written or verbal warnings or instant dismissal in circumstances that amount to gross misconduct.

13.2 The College reserves the right to take appropriate disciplinary action against contractors and self-employed service providers who fail to comply with this policy. Such actions include, but are not limited to, the termination of any contract with the College.

Appendix 1 – UK GDPR Definitions

Child – in the United Kingdom of Great Britain and Northern Ireland, the processing of personal data of a child under the age 13, in relation to 'Information Society Services', is only lawful if the consent of the person with parental responsibility has been obtained. The controller shall make reasonable efforts to verify that consent is given or authorised by the person who is the holder of parental responsibility over the child.

Data controller – the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law.

Data subject – any living individual who is the subject of personal data held by an organisation.

Data subject consent - means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data.

Establishment – the main establishment of the controller in the EU will be the place in which the controller makes the main decisions as to the purpose and means of its data processing activities. The main establishment of a processor in the EU will be its administrative centre. If a controller is based outside the EU, it will have to appoint a representative in the jurisdiction in which the controller operates to act on behalf of the controller and deal with supervisory authorities.

Filing system – any structured set of personal data which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis.

Personal data – any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Personal data breach – a breach of security leading to the accidental, or unlawful, destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed. There is an obligation on the controller to report personal data breaches to the supervisory authority and where the breach is likely to adversely affect the personal data or privacy of the data subject.

Processing – any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Profiling – is any form of automated processing of personal data intended to evaluate certain personal aspects relating to a natural person, or to analyse or predict that person's performance at work, economic situation, location, health, personal preferences, reliability, or behaviour. This definition is linked to the right of the data subject to object to profiling and a right to be informed about the existence of profiling, of measures based on profiling and the envisaged effects of profiling on the individual.

Special categories of personal data – personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade-union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

Third party – a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data.